

Rational Invariant Theory

Harm Derksen
University of Michigan

subfields \Leftrightarrow ideals

Let K be a field and $L : K$ be a finitely generated field extension (a *function field*). For simplicity, we take $K = \mathbf{C}$ and $L = \mathbf{C}(\mathbf{x}) := \mathbf{C}(x_1, \dots, x_n)$. Consider the Noetherian ring

$$\mathbf{C}(\mathbf{x}) \otimes_{\mathbf{C}} \mathbf{C}(\mathbf{y}) = \left\{ \frac{f(\mathbf{x}, \mathbf{y})}{g_1(\mathbf{x})g_2(\mathbf{y})} \mid f, g_1, g_2 \text{ poly's} \right\} \subseteq \mathbf{C}(\mathbf{x}, \mathbf{y})$$

An ideal

$$\mathbf{b} = (h_1(\mathbf{x}, \mathbf{y}), \dots, h_r(\mathbf{x}, \mathbf{y})) \subseteq \mathbf{C}(\mathbf{x}) \otimes_{\mathbf{C}} \mathbf{C}(\mathbf{y})$$

is a *coideal* or an *equivalence relation ideal* if it satisfies

reflexive: $h_i(\mathbf{x}, \mathbf{x}) = 0$ for all i ;

symmetric: $\mathbf{b} = (h_1(\mathbf{y}, \mathbf{x}), \dots, h_r(\mathbf{y}, \mathbf{x}))$;

transitive: For all i , $h_i(\mathbf{x}, \mathbf{y}) \in \mathbf{C}(\mathbf{x}) \otimes_{\mathbf{C}} \mathbf{C}(\mathbf{z}) \otimes_{\mathbf{C}} \mathbf{C}(\mathbf{y})$
lies in

$$(h_1(\mathbf{x}, \mathbf{z}), \dots, h_r(\mathbf{x}, \mathbf{z})) + (h_1(\mathbf{z}, \mathbf{y}), \dots, h_r(\mathbf{z}, \mathbf{y})).$$

(think of \mathbf{b} as vanishing ideal of an equivalence relation)

reflexive + transitive \Rightarrow symmetric

Example: $\mathbf{C} \subseteq M \subseteq \mathbf{C}(\mathbf{x})$ intermediate field. Then

$$\mathbf{a}(M) := (f(\mathbf{x}) - f(\mathbf{y}) \mid f(\mathbf{x}) \in M) \subseteq \mathbf{C}(\mathbf{x}) \otimes_{\mathbf{C}} \mathbf{C}(\mathbf{y})$$

is a coideal.

Theorem (Sweedler): These are the *only* examples, so coideals in $\mathbf{C}(\mathbf{x}) \otimes_{\mathbf{C}} \mathbf{C}(\mathbf{y}) \Leftrightarrow$ int. fields $\mathbf{C} \subseteq M \subseteq \mathbf{C}(\mathbf{x})$

Goal: Translate computational problems for fields into computational problems for ideals and use Gröbner bases.

Problem: Given coideal $\mathbf{a} \subseteq \mathbf{C}(\mathbf{x}) \otimes_{\mathbf{C}} \mathbf{C}(\mathbf{y})$, how to compute generators of a field M such that $\mathbf{a} = \mathbf{a}(M)$.

1. Compute $\mathbf{b} := \mathbf{a} \cap \mathbf{C}(\mathbf{x})[\mathbf{y}]$ (???)
2. Compute reduced Gröbner basis G of \mathbf{b} .
3. Then M is the field generated by all coefficients of all elements of \mathcal{G} .

Problem: Given an ideal

$$\mathbf{a} = (h_1(\mathbf{x}, \mathbf{y}), \dots, h_r(\mathbf{x}, \mathbf{y})) \subseteq \mathbf{C}(\mathbf{x}) \otimes_{\mathbf{C}} \mathbf{C}(\mathbf{y}),$$

compute $\mathbf{a} \cap \mathbf{C}(\mathbf{x})[\mathbf{y}]$. Without loss of generality, $h_i(\mathbf{x}, \mathbf{y}) \in \mathbf{C}(\mathbf{y})[\mathbf{x}]$ for all i .

1. Let $\mathbf{c} \subseteq \mathbf{C}(\mathbf{y})[\mathbf{x}]$ be the ideal generated $h_1(\mathbf{x}, \mathbf{y}), \dots, h_r(\mathbf{x}, \mathbf{y})$.
2. Compute $\mathbf{d} = \mathbf{c} \cap \mathbf{C}[\mathbf{x}, \mathbf{y}]$ (???)
3. Then $\mathbf{b} = \mathbf{a} \cap \mathbf{C}(\mathbf{x})[\mathbf{y}]$ is the ideal generated by \mathbf{d} .

Problem: Given an ideal $\mathbf{c} \subseteq \mathbf{C}(\mathbf{y})[\mathbf{x}]$, compute $\mathbf{d} = \mathbf{c} \cap \mathbf{C}[\mathbf{x}, \mathbf{y}]$.

1. Compute Gröbner basis $G = \{u_1(\mathbf{x}, \mathbf{y}), \dots, u_r(\mathbf{x}, \mathbf{y})\}$ of \mathbf{c} .
2. Find $p(\mathbf{y}) \in \mathbf{C}[\mathbf{y}]$ such that $p(\mathbf{y})u_i(\mathbf{x}, \mathbf{y}) \in \mathbf{C}[\mathbf{x}, \mathbf{y}]$.
3. Then $\mathbf{d} = ((p(\mathbf{y})u_1(\mathbf{x}, \mathbf{y}), \dots, p(\mathbf{y})u_r(\mathbf{x}, \mathbf{y})) : p(\mathbf{y})^\infty)$.

Note: $(I : p(\mathbf{x})^\infty) = (I + (zp(\mathbf{x}) - 1)) \cap \mathbf{C}[\mathbf{x}, z]$ for any ideal $I \subseteq \mathbf{C}[\mathbf{x}]$. (Use Gröbner elimination.)

Given an ideal $\mathbf{c} \subseteq \mathbf{C}(\mathbf{y})[\mathbf{x}]$, one can compute $\mathbf{c} \cap \mathbf{C}[\mathbf{x}]$ by intersecting $\mathbf{d} := \mathbf{c} \cap \mathbf{C}[\mathbf{x}, \mathbf{y}]$ with $\mathbf{C}[\mathbf{x}]$ using Gröbner elimination.

(Trivial) Example: The ideal

$$\mathbf{a} = (x_1x_2 - y_1y_2, x_2^2 - x_2y_1 - x_2y_2 + y_1y_2)$$

of $\mathbf{C}(x_1, x_2) \otimes_{\mathbf{C}} \mathbf{C}(y_1, y_2)$ is a coideal. Define

$$\mathbf{c} = (x_1x_2 - y_1y_2, x_2^2 - x_2y_1 - x_2y_2 + y_1y_2)$$

in $\mathbf{C}(y_1, y_2)[x_1, x_2]$. A reduced Gröbner basis of \mathbf{c} is

$$\{x_1 + x_2 - y_1 - y_2, x_2^2 - x_2y_1 - x_2y_2 + y_1y_2\}$$

Fortunately, all elements lie in $\mathbf{C}[x_1, x_2, y_1, y_2]$ already which means that we do not have to compute the colon ideal, so

$$\mathbf{d} = (x_1 + x_2 - y_1 - y_2, x_2^2 - x_2y_1 - x_2y_2 + y_1y_2)$$

in $\mathbf{C}[x_1, x_2, y_1, y_2]$. Now finally

$$\mathbf{b} = (x_1 + x_2 - y_1 - y_2, x_2^2 - x_2y_1 - x_2y_2 + y_1y_2)$$

in $\mathbf{C}(x_1, x_2)[y_1, y_2]$ is equal to $\mathbf{a} \cap \mathbf{C}(x_1, x_2)[y_1, y_2]$. A Gröbner basis of \mathbf{b} is:

$$\begin{aligned} \mathbf{b} &= \{y_1 + y_2 - x_1 - x_2, y_2^2 - y_2x_1 - y_2x_2 + x_1x_2\} = \\ &= \{y_1 + y_2 - (x_1 + x_2), y_2^2 - y_2(x_1 + x_2) + x_1x_2\} \end{aligned}$$

Taking coefficients shows that $\mathbf{a} = \mathbf{a}(M)$ where $M = \mathbf{C}(x_1 + x_2, x_1x_2)$.

Algorithms for function fields

(After Beth, Müller-Quade, Steinwandt.) Let $\mathbf{C} \subseteq M \subseteq \mathbf{C}(\mathbf{x})$ be an intermediate field. Define $\mathbf{a}(M) \subseteq \mathbf{C}(\mathbf{x}) \otimes_{\mathbf{C}} \mathbf{C}(\mathbf{y})$ as before,

$$\mathbf{b}(M) = \mathbf{a}(M) \cap \mathbf{C}(\mathbf{x})[\mathbf{y}]$$

and let $\mathcal{G}(M)$ be a reduced Gröbner basis of $\mathbf{b}(M)$.

Membership: $u(\mathbf{x}) = f(\mathbf{x})/g(\mathbf{x}) \in M$ if and only if

$$f(\mathbf{y}) - u(\mathbf{x})g(\mathbf{y})$$

reduces to 0 modulo $\mathcal{G}(M)$.

Field comparison: $M_1 = M_2 \Leftrightarrow \mathcal{G}(M_1) = \mathcal{G}(M_2)$.

Canonical generators: Coefficients of $\mathcal{G}(M)$ form canonical field generators of M . Every element of M can be easily expressed in these using the Membership algorithm.

Rational invariants: Let G be a connected algebraic group acting regularly on \mathbf{C}^n . Then it acts also on $\mathbf{C}(\mathbf{x})$. Let $\mathbf{C}(\mathbf{x})^G$ be the field of invariant rational functions.

Let $\psi : G \times \mathbf{C}^n \rightarrow \mathbf{C}^n \times \mathbf{C}^n$ be the “graph morphism” defined by $(g, v) \mapsto (v, g \cdot v)$. This corresponds to a homomorphism

$$\psi^* : \mathbf{C}[\mathbf{x}, \mathbf{y}] \rightarrow \mathbf{C}[G] \otimes_{\mathbf{C}} \mathbf{C}[\mathbf{x}],$$

where $\mathbf{C}[G]$ is the affine coordinate ring of G . This extends to

$$\psi^* : \mathbf{C}(\mathbf{x})[\mathbf{y}] \rightarrow \mathbf{C}[G] \otimes_{\mathbf{C}} \mathbf{C}(\mathbf{x}) \cong \mathbf{C}(\mathbf{x})[G].$$

Compute the kernel $\ker(\psi^*)$ with Gröbner bases methods. We have

$$\ker(\psi^*) = \mathbf{b}(\mathbf{C}(\mathbf{x})^G).$$

Now generators of $\mathbf{C}(\mathbf{x})^G$ can be computed by computing a reduced Groebner basis of $\mathbf{b}(\mathbf{C}(\mathbf{x})^G)$ and taking all coefficients.

Intersection fields

Suppose that $M_1, M_2 \subseteq \mathbf{C}(\mathbf{x})$ are subfields, algebraically closed in $\mathbf{C}(\mathbf{x})$. The ideal

$$\mathfrak{p} = (\mathfrak{a}(M_1)^{(\mathbf{x}, \mathbf{z})} + \mathfrak{a}(M_2)^{(\mathbf{z}, \mathbf{y})}) \cap \mathbf{C}(\mathbf{x}) \otimes_{\mathbf{C}} \mathbf{C}(\mathbf{y})$$

in $\mathbf{C}(\mathbf{x}) \otimes_{\mathbf{C}} \mathbf{C}(\mathbf{z}) \otimes_{\mathbf{C}} \mathbf{C}(\mathbf{y})$ is prime. Now take the transitive closure: Define $\mathfrak{p}_0 := \mathfrak{p}$ and

$$\mathfrak{p}_{n+1} = (\mathfrak{p}_n^{(\mathbf{x}, \mathbf{z})} + \mathfrak{p}_n^{(\mathbf{z}, \mathbf{y})}) \cap \mathbf{C}(\mathbf{x}) \otimes_{\mathbf{C}} \mathbf{C}(\mathbf{y})$$

in $\mathbf{C}(\mathbf{x}) \otimes_{\mathbf{C}} \mathbf{C}(\mathbf{z}) \otimes_{\mathbf{C}} \mathbf{C}(\mathbf{y})$ for $n \geq 1$. The sequence

$$\mathfrak{p}_0 \supseteq \mathfrak{p}_1 \supseteq \mathfrak{p}_2 \supseteq \cdots$$

prime ideals must stabilize because of dimension:

$$\mathfrak{q} := \mathfrak{p}_m = \mathfrak{p}_{m+1} = \mathfrak{p}_{m+2} = \cdots$$

for some m . Then $\mathfrak{q} = \mathfrak{a}(M_1 \cap M_2)$. This idea can be made into an algorithm to compute $M_1 \cap M_2$.

Remarks

All the algorithms so far are not fast. Most of them need Gröbner bases algorithms over polynomial rings in many variables over basefield which are a function fields.

However, all algorithms generalize to *arbitrary* fields of *arbitrary* characteristic. Also, they generalize to arbitrary function fields (instead of just *rational function fields*).

Faster, more heuristic methods in characteristic 0 will be discussed later.

Theoretical Applications

Quotients of equivalence relations. Suppose that $R \subseteq \mathbf{C}^n \times \mathbf{C}^n$ is an equivalence relation and a constructible set (union of locally closed subvarieties). Does there exist a morphism $\phi : \mathbf{C}^n \rightarrow Y$ of affine varieties such that every equivalence class is a fiber $\phi^{-1}(y)$ for some $y \in Y$? Answer: No, not even if R is Zariski closed. (For example Finston-Deveney, $n = 5$, where equivalence classes are orbits of an additive group action.) However:

Theorem: There exists a dense Zariski open subset $U \subseteq \mathbf{C}^n$ and a morphism of affine varieties $\phi : U \rightarrow Y$ such that the nonempty fibers of ϕ are exactly all equivalence classes (intersected with U).

(Similar results seem to be known. For example, M. Artin has a similar result “buried” in the language of algebraic spaces.)

In positive characteristic one needs slightly stronger assumptions.

Discrete polynomial dynamical systems. Suppose that $\sigma : \mathbf{C}^n \rightarrow \mathbf{C}^n$ is a dominant polynomial map. Let

$$\mathbf{C}(\mathbf{x})^\sigma = \{f(\mathbf{x}) \in \mathbf{C}(\mathbf{x}) \mid f(\sigma(\mathbf{x})) = f(\mathbf{x})\}$$

be the field of rational invariants.

For $v \in \mathbf{C}^n$, let $\overline{O}(v)$ be the Zariski closure of

$$\{v, \sigma(v), \sigma^2(v), \dots\}.$$

Theorem: The function $\dim \overline{O}(v)$ is maximal outside some countable union of Zariski closed (proper) subsets. This maximal value is equal to the transcendence degree of $\mathbf{C}(\mathbf{x}) : \mathbf{C}(\mathbf{x})^\sigma$.

Corollary: There exist nontrivial rational invariants if and only if $\{v, \sigma(v), \sigma^2(v), \dots\}$ is not Zariski dense in \mathbf{C}^n for all $v \in \mathbf{C}^n$.

Similar results hold for continuous polynomial dynamical systems (systems of polynomial differential equations).

Derivations

Let $\text{Der}_{\mathbf{C}}(\mathbf{C}(\mathbf{x}))$ be the set of all derivations of $\mathbf{C}(\mathbf{x})$ over \mathbf{C} . Every element of $\text{Der}_{\mathbf{C}}(\mathbf{C}(\mathbf{x}))$ is of the form:

$$D = a_1(\mathbf{x}) \frac{\partial}{\partial x_1} + a_2(\mathbf{x}) \frac{\partial}{\partial x_2} + \cdots + a_n(\mathbf{x}) \frac{\partial}{\partial x_n} \quad (1)$$

with $a_1(\mathbf{x}), \dots, a_n(\mathbf{x}) \in \mathbf{C}(\mathbf{x})$.

$\text{Der}_{\mathbf{C}}(\mathbf{C}(\mathbf{x}))$ is a Lie algebra. If $D, E \in \text{Der}_{\mathbf{C}}(\mathbf{C}(\mathbf{x}))$ then $[D, E] := DE - ED \in \text{Der}_{\mathbf{C}}(\mathbf{C}(\mathbf{x}))$. Moreover, $\text{Der}_{\mathbf{C}}(\mathbf{C}(\mathbf{x}))$ is an n -dimensional $\mathbf{C}(\mathbf{x})$ -vector space. To a derivation (1) we may associate a system of differential equations:

$$\left\{ \begin{array}{l} \dot{x}_1(t) = a_1(\mathbf{x}(t)) \\ \dot{x}_2(t) = a_2(\mathbf{x}(t)) \\ \vdots \quad \quad \quad \vdots \\ \dot{x}_n(t) = a_n(\mathbf{x}(t)) \end{array} \right.$$

By the chain rule: $f(x_1(t), \dots, x_n(t))$ is constant for every initial conditions for $\mathbf{x}(0)$ if and only if $Df(\mathbf{x}) = 0$. Such a $f(\mathbf{x})$ is sometimes called a rational first integral.

For an intermediate field $\mathbf{C} \subseteq M \subseteq \mathbf{C}(\mathbf{x})$, one has

$$\text{Der}_M(\mathbf{C}(\mathbf{x})) = \{D \in \text{Der}_{\mathbf{C}}(\mathbf{C}(\mathbf{x})) \mid Df(\mathbf{x}) = 0 \forall f(\mathbf{x}) \in M\}$$

For a set of derivations \mathcal{L} , define

$$\mathbf{C}(\mathbf{x})^{\mathcal{L}} = \{f(\mathbf{x}) \in \mathbf{C}(\mathbf{x}) \mid Df(\mathbf{x}) = 0 \forall f \in \mathcal{L}\}.$$

Then $\mathbf{C}(\mathbf{x})^{\text{Der}_M(\mathbf{C}(\mathbf{x}))}$ is the set of all elements of $\mathbf{C}(\mathbf{x})$ which are algebraic over M .

Theorem. If $\mathbf{C} \subseteq M_1, M_2 \subseteq \mathbf{C}(\mathbf{x})$ are two intermediate fields which are algebraically closed in $\mathbf{C}(\mathbf{x})$, then $\text{Der}_{M_1 \cap M_2}(\mathbf{C}(\mathbf{x}))$ is the Lie algebra generated by $\text{Der}_{M_1}(\mathbf{C}(\mathbf{x}))$ and $\text{Der}_{M_2}(\mathbf{C}(\mathbf{x}))$.

For intermediate fields $M_1, M_2 \subseteq \mathbf{C}(\mathbf{x})$ which are algebraically closed in $\mathbf{C}(\mathbf{x})$ we can compute $M_1 \cap M_2$ as follows:

1. Compute $\text{Der}_{M_1}(\mathbf{C}(\mathbf{x})), \text{Der}_{M_2}(\mathbf{C}(\mathbf{x}))$ (linear algebra);
2. Compute the Lie algebra \mathcal{L} generated by $\text{Der}_{M_1}(\mathbf{C}(\mathbf{x}))$ and $\text{Der}_{M_2}(\mathbf{C}(\mathbf{x}))$ (more linear algebra).
3. Compute $\mathbf{C}(\mathbf{x})^{\mathcal{L}}$ (???)

In step 2 we computed $\text{Der}_{M_1 \cap M_2}(\mathbf{C}(\mathbf{x}))$. We have that

$$\dim_{\mathbf{C}(\mathbf{x})}(\text{Der}_{M_1 \cap M_2}(\mathbf{C}(\mathbf{x})))$$

is equal to the transcendence degree of $\mathbf{C}(\mathbf{x}) : M_1 \cap M_2$.

In step 3 we search for elements in $\mathbf{C}(\mathbf{x})^{\mathcal{L}}$ until we have enough algebraically independent elements to form a transcendence basis of $M_1 \cap M_2$ over \mathbf{C} . After that generators of $M_1 \cap M_2$ can be found using a (time-consuming) algorithm of Vasconcelos.

Problem: How to search efficiently for nontrivial elements of $\mathbf{C}(\mathbf{x})^{\mathcal{L}}$?

Such an efficient method does exist. We will discuss the case where \mathcal{L} is just one derivation.

Constants of derivations

Suppose that D is a derivation of $\mathbf{C}(\mathbf{x})$ over \mathbf{C} . Let m_1, m_2, m_3, \dots be the sequence of all monomials in $\mathbf{C}[\mathbf{x}]$. Define the Wronsky matrix

$$W_d := \begin{pmatrix} m_1 & m_2 & \cdots & m_d \\ Dm_1 & Dm_2 & \cdots & Dm_d \\ \vdots & \vdots & \ddots & \vdots \\ D^{d-1}m_1 & D^{d-1}m_2 & \cdots & D^{d-1}m_d \end{pmatrix}$$

Proposition. $\mathbf{C}(\mathbf{x})^D \neq \mathbf{C}$ if and only if $\det(W_d) = 0$ for some d . Suppose d is minimal with $\det(W_d) = 0$. Then there exist *unique* $f_1(\mathbf{x}), \dots, f_{d-1}(\mathbf{x}) \in \mathbf{C}(\mathbf{x})$ with:

$$W_d \cdot \begin{pmatrix} f_1(\mathbf{x}) \\ f_2(\mathbf{x}) \\ \vdots \\ f_{d-1}(\mathbf{x}) \\ 1 \end{pmatrix} = 0.$$

Then $f_1(\mathbf{x}), \dots, f_d(\mathbf{x}) \in \mathbf{C}(\mathbf{x})^D$, and not all constant.

Repeating this one finds generators of $\mathbf{C}(\mathbf{x})^D$ eventually.

(Trivial) Example: Let

$$D = x_1 \frac{\partial}{\partial x_1} + (2x_2 + x_1 + 2) \frac{\partial}{\partial x_2}$$

We list the monomials (in increasing total degree ordering with $x_2 > x_1$):

$$1, x_1, x_2, x_1^2, x_1x_2, x_2^2, \dots$$

The smallest d for which $\det(W_d) = 0$ is $d = 4$:

$$W_4 = \begin{pmatrix} 1 & x_1 & x_2 & x_1^2 \\ 0 & x_1 & 2x_2 + x_1 + 2 & 2x_1^2 \\ 0 & x_1 & 4x_2 + 3x_1 + 4 & 4x_1^2 \\ 0 & x_1 & 8x_2 + 7x_1 + 8 & 8x_1^2 \end{pmatrix}$$

Solving $W_4 \cdot v = 0$ with last coordinate of v equal to 1 yields

$$v = \begin{pmatrix} -t \\ -t \\ -t \\ 1 \end{pmatrix}$$

Where $t = \frac{x_1^2}{1 + x_1 + x_2} \in \mathbf{C}(x_1, x_2)^D$.

With similar methods one can:

- find limit cycles or nontrivial differential ideals
- find algebraic equations if for given initial conditions the flow is contained in a Zariski closed subset.
- find algebraic solutions for polynomial differential equations.
- for polynomial differential equations with parameters one can search for special values of those parameter for which there exist rational first integrals
- find invariants for discrete polynomial dynamical systems
- find equations for $\overline{O}(v)$ for any discrete polynomial dynamical systems where $v \in \mathbf{C}^n$ etc.

Remark: The number of algebraically independent rational first integrals can only go up after a degeneration of the polynomial differential equation. This can be used in some cases to prove the non-existence of rational first integrals.